Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 23 août 2013
N° CERTA-2013-ACT-034

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-034

1 Bogue dans un correctif de Microsoft

Microsoft a diffusé la semaine dernière un correctif visant à pallier la vulnérabilité MS13-061 dans Exchange. Un effet de bord de cette mise à jour désactive les fonctions d'indexation du serveur de messagerie.

L'éditeur travaille actuellement sur une nouvelle version de ce correctif, et propose dans l'intervalle des mesures permettant de pallier ses effets négatifs.

Le CERTA rappelle l'importance d'une validation des mises à jour avant leur déploiement, et recommande une surveillance accrue des sites des éditeurs dans les jours qui suivent la publication de mises à jour, afin d'être en mesure de faire face dans les meilleurs délais à d'éventuels dysfonctionnements observés.

Documentation

- Avis CERTA-2013-AVI-472 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-472/
- Bulletin de support Microsoft pour rétablir l'indexation Exchange :
  http://support.microsoft.com/kb/2879739

2 Vulnérabilité critique dans *Joomla!*

Une vulnérabilité particulièrement critique a récemment été corrigée dans *Joomla!*. Évoquée dans l'avis CERTA-2013-AVI-460, la vulnérabilité se trouve dans le composant « Media Manager » de *Joomla!*. Ce composant permet à l'origine de téléverser certains types de fichiers autorisés, comme des images. Le filtrage pour autoriser ou non le dépôt d'un fichier est basé sur l'extension du fichier. Or ce filtrage était mal effectué et il était possible de téléverser un fichier arbitraire avec un nom se terminant par le caractère « . », par exemple « fichier.php. ».

Il est ensuite possible d'accéder aux fichiers ainsi téléversés par l'intermédiaire du serveur Web. Dans le cas du serveur Web « Apache », il faut savoir que les extensions non reconnues sont ignorées et c'est l'extension reconnue la plus à droite dans le nom du fichier qui est prise en compte. Avec l'exemple « fichier.php. », le fichier est donc interprété en tant que fichier PHP par « Apache » et permet d'exécuter du code arbitraire sur le serveur Web.

Les versions affectées de *Joomla!* sont celles antérieures à 2.5.14 pour la branche 2.5.x et antérieures à 3.1.5 pour la branche 3.x. Il est nécessaire de faire une mise à jour le plus rapidement possible.

D'une manière générale, le CERTA souligne l'importance de tenir à jour les gestionnaires de contenu. En effet, le CERTA a constaté que parmi les attaquants pratiquant la défiguration de sites Internet, beaucoup visent particulièrement ces produits, car les méthodes d'attaques sur ces gestionnaires sont généralement simples et documentées, et des outils d'exploitation sont facilement accessibles.

Documentation

- Avis CERTA-2013-AVI-460 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-460/
- Bulletin de sécurité *Joomla!* du 31 juillet 2013 :
  http://developer.joomla.org/security/news/563-20130801-core-unauthorised-uploads

3 Envoi d'exécutables malveillants par courriel

De nombreux incidents traités par le CERTA ont pour origine des courriels malveillants. Souvent, de simples exécutables malveillants sont envoyés en pièce jointe et traversent pourtant l'ensemble des dispositifs de sécurité mis en place.

Si la malveillance de ces courriels est généralement assez facilement identifiable par leur contenu négligé (fautes d'orthographe, français approximatif, *etc.*), certains attaquants sont plus subtils. Récemment, le CERTA a eu affaire à une vague de messages où le nom et le prénom de l'utilisateur étaient inscrits dans le nom d'un exécutable malveillant en pièce jointe, faisant croire à ce dernier qu'il était directement concerné par le sujet pour l'inciter à l'ouvrir.

Outre la sensibilisation des utilisateurs à ce genre d'attaques, quelques mesures permettent de s'en prémunir :

- le blocage des fichiers de type exécutable, y compris lorsqu'ils sont compressés, au niveau du serveur de messagerie est la solution la plus simple à mettre en œuvre. Cette recommandation peut aussi s'appliquer aux serveurs mandataires HTTP ;
- la mise en place des stratégies de restriction logicielles (SRP), ou d'*AppLocker* à partir de Windows Vista, sur les postes de travail protège non seulement de ce type d'attaques, mais aussi de nombreux logiciels malveillants circulant sur Internet.

Documentation

- Guide de configuration des stratégies de restriction logicielles :
  http://technet.microsoft.com/library/cc163080.aspx
- Guide de configuration de *AppLocker* :
  http://technet.microsoft.com/library/dd723678.aspx

4 Rappel des avis émis

Dans la période du 16 au 22 août 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-478 : Multiples vulnérabilités dans PHP
- CERTA-2013-AVI-479 : Vulnérabilité dans le système SCADA Kepware Technologies KEPServerEX
- CERTA-2013-AVI-480 : Vulnérabilité dans le système SCADA Advantech WebAccess
- CERTA-2013-AVI-481 : Multiples vulnérabilités dans le système SCADA Tridium Niagara
- CERTA-2013-AVI-482 : Multiples vulnérabilités dans Puppet
- CERTA-2013-AVI-483 : Vulnérabilité dans le système SCADA Schneider Electric Trio Radio
- CERTA-2013-AVI-484 : Vulnérabilité dans Xen
- CERTA-2013-AVI-485 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
- CERTA-2013-AVI-486 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-487 : Vulnérabilité dans Check Point
- CERTA-2013-AVI-488 : Vulnérabilité dans EMC RSA
- CERTA-2013-AVI-489 : Multiples vulnérabilités dans Cisco Unified Communications Manager
- CERTA-2013-AVI-490 : Vulnérabilité dans Cisco Unified Communications Manager IM et Presence Service
- CERTA-2013-AVI-491 : Multiples vulnérabilités dans Cisco Prime Central

Gestion détaillée du document

23 août 2013 version initiale.